P06 – Relatório de Funcionalidades

pwc strategy&

(DC2) Uso Restrito na PwC - Confidencial

Projeto de Auditoria e Consultoria para Revisão, Definição e Implantação de Modelo de Auditoria e Fiscalização dos Contratos e Avaliação Estratégica do Sistema de Ônibus

RIO PREFEITURA

Dezembro de 2014

Etapa 2 - Auditoria do Sistema de Bilhetagem Eletrônica (SBE)

P06 – Relatório de Funcionalidades

pwc

Rio de Janeiro, 3 de dezembro de 2014.

À
Secretaria Municipal de Transporte
Prefeitura da Cidade do Rio de Janeiro

Atenção: V. Exª. Sr. Alexandre Sansão Fontes
Secretário Municipal de Transportes do Rio de Janeiro

Prezado Senhor:

De acordo com Termo de Referência referente à Etapa 2 do Projeto de Projeto de Auditoria e Consultoria para Revisão, Definição e Implantação de Modelo de Auditoria e Fiscalização dos Contratos e Avaliação Estratégica do Sistema de Ônibus, apresentamos a seguir nosso Relatório de Funcionalidades.

Nossos trabalhos consistiram na realização de uma série de testes no ambiente tecnológico da RioCard, responsável pelo processo de bilhetagem eletrônica do Município do Estado do Rio de Janeiro, durante o período de 04 de agosto à 30 de novembro de2014. Como resultado, elaboramos um relatório detalhado contendo a abordagem adotada, resultados obtidos e recomendações sugeridas; não abrangendo, portanto, procedimentos orientados aos exames das demonstrações financeiras, de responsabilidade dos auditores externos. Assim, não estaremos em condições de emitir, e não emitiremos, parecer sobre as suas demonstrações financeiras e sobre os processos objetos de nossa revisão.

A PwC não assume qualquer responsabilidade para com terceiros em relação aos resultados aqui reportados.

Ressaltamos que nossos trabalhos não esgotam futuras análises ou revisões específicas e mais amplas que poderão, eventualmente, identificar outros aspectos de melhoria.

Permanecemos à disposição para quaisquer esclarecimentos.

Atenciosamente,

Ronaldo Matos Valiño
PRICEWATERHOUSECOOPERS

Conteúdo

1. Introdução 4
2. Abordagem e Etapas do Projeto 6
3. Escopo e Regras de Negócios 9
4. Resultados Obtidos 11
   - 4.1. Análise das funcionalidades do Sistema de Bilhetagem Eletrônica (SBE) e Validador 11
   - 4.1.1. Análise da usabilidade do Sistema de Bilhetagem Eletrônica (SBE) 11
   - 4.2. Análise de Treinamento 24
   - 4.3. Análise da documentação existente do Sistema de Bilhetagem Eletrônica (SBE) 26
   - 4.4. Identificação e análise dos acordos de níveis de serviços (SLA) existentes para o suporte técnico do Sistema de Bilhetagem Eletrônica (SBE) 36
   - 4.5. Análise do Sistema Validador 41
   - 4.5.1. Identificação e Análise dos controles existentes no Sistema Validador 44
5. Distorções/Divergências identificadas e recomendações sugeridas 49
   - 5.1. Identificação e Análise dos controles existentes que garantam integridade e autenticidade das informações de usuários do Sistema de Bilhete Único (BU) 49
   - 5.2. Identificação e Análise dos controles existentes que garantam integridade e autenticidade das informações de passagens, recargas de bilhetes, e pagamentos realizados pela RioCard 53

Anexo A - Glossário 54

1. Introdução

Este relatório é parte integrante da **Etapa 2** do projeto de **Auditoria e Consultoria para Revisão, Definição e Implantação de Modelo de Auditoria e Fiscalização dos Contratos e Avaliação Estratégica do Sistema de Ônibus**, que contempla três produtos (relatórios) em sua totalidade, sendo eles:

- ✓ P04 - Relatório de Avaliação das Regras de Negócio;
- ✓ P05 - Relatório da Segurança do Sistema de Bilhetagem Eletrônica (SBE); e
- ✓ P06 - Relatório de Funcionalidades.

O relatório em questão (P06) possui como objetivo avaliar às funcionalidades do Sistema de Bilhetagem Eletrônica (SBE) e do Validador que estão em operação.

Desta forma, conforme definido no referido Termo de Referência, as seguintes atividades fizeram parte do escopo de nosso trabalho:

1. Análise da ***usabilidade*** do Sistema de Bilhetagem Eletrônica (SBE);
2. Análise dos ***treinamentos***, considerando: material e processo existente e quantidade de usuários treinados;
3. Análise da ***documentação existente*** do Sistema de Bilhetagem Eletrônica (SBE), tanto em nível de usuários, quanto em nível técnico;
4. Identificação e Análise dos ***serviços e acordos de SLAs*** (níveis de acordo de serviços) existentes para o suporte técnico do Sistema de Bilhetagem Eletrônica (SBE);
5. Identificação e Análise dos controles existentes que garantam ***integridade e autenticidade das informações de usuários*** do ***Sistema de Bilhete Único (BU)***;
6. Identificação e Análise dos controles existentes que garantam a ***integridade e autenticidade das informações de passagens***;

7. Identificação e Análise dos controles existentes que garantam a ***integridade e autenticidade das informações de recargas de bilhetes***;

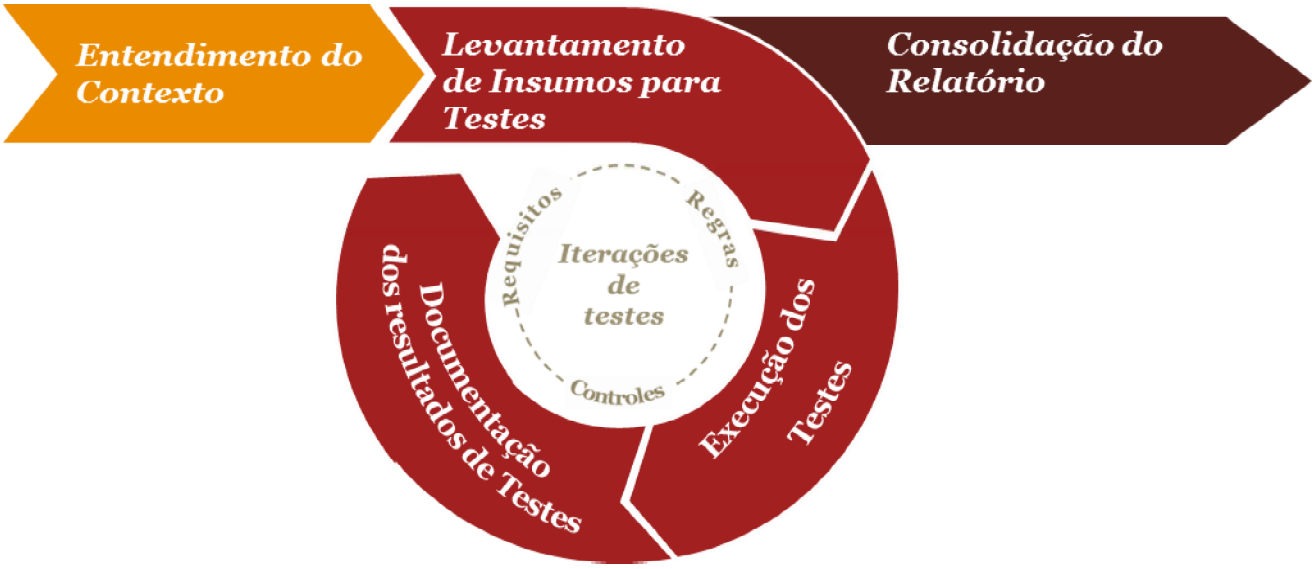
8. Identificação e Análise dos controles existentes que garantam a ***integridade e autenticidade das informações dos pagamentos*** realizados pela RioCard; e

9. Identificação e Análise dos controles existentes no ***Sistema Validador*** que garantam:
   9.1 Integridade e autenticidade das informações do ***cartão***;
   9.2 Integridade e autenticidade das informações de ***passagens***;
   9.3 Integridade e autenticidade das informações do ***validador***;
   9.4 Integridade e autenticidade das informações de ***recargas***;
   9.5 Integridade e autenticidade do ***código dos sistemas***;

2. Abordagem e Etapas do Projeto

Para atender os objetivos definidos para esse relatório, adotamos a abordagem segregada nas etapas abaixo e demonstradas na ***Figura 1***:

Figura 1 – Etapas do Projeto



I. Entendimento do Contexto

Nesta etapa foram realizados o levantamento e o entendimento do contexto relacionado às funcionalidades do Sistema de Bilhetagem Eletrônica (SBE) e do Validador que se estão em operação. Desta forma, executamos as seguintes atividades:

(a) Preparação da documentação de solicitação de informações;

(b) Envio de documentos de preparação de roteiro de entrevistas, bem como definição de datas de entrevistas a serem realizadas com os gestores responsáveis;

(c) Obtenção de documentação preliminar com base em resultado das entrevistas realizadas; e

(d) Análise de documentação recebida.

II. Levantamento de insumos para testes

Nesta etapa foram realizadas entrevistas de aprofundamento de entendimento a respeito de cada um dos itens a serem avaliados. Para isto, as seguintes atividades foram executadas:

(a) Acompanhamento das atividades e controles realizados (processo de *walkthrough*);

(b) Documentação do entendimento do processo realizado no item (a) acima;

(c) Definição das necessidades de informações para realização dos testes (necessidades de evidências);

(d) Elaboração dos Planos de Testes; e

(e) Envio da solicitação de informações para realização dos testes.

III. Execução dos testes

Nesta etapa foram executados os Planos de Testes, definidos e documentados na Etapa anterior, com o objetivo de confirmar a aderência dos controles identificados. Para isto, as seguintes atividades foram executadas:

(a) Execução dos Planos de Testes, sendo que o período de nossos testes compreendeu o intervalo de 01.01.2014 até data da realização do referido teste, que foram realizados ao longo do 2º semestre de 2014; e

(b) Documentação dos resultados obtidos.

IV. Documentação dos resultados dos testes

Nesta etapa foram realizadas as análises dos resultados dos testes, bem como a elaboração de recomendações nos casos de identificação de deficiências ou sugestão de melhorias ao processo analisado. Para isto, executamos as seguintes atividades:

(a) Análise dos resultados dos testes;

(b) Consolidação da documentação de resultado dos testes;

(c) Confirmação dos resultados dos testes; e

(d) Elaboração de recomendações de melhoria.

V. Consolidação do Relatório

Após a execução de todas as análises previstas para cada frente de trabalho, consolidamos os produtos finais previstos pelo projeto. Para isto, executamos as seguintes atividades:

(a) Consolidação das avaliações de cada frente de trabalho;

(b) Apresentação dos resultados através da execução de *workshops* técnicos de validação dos resultados;

(c) Elaboração do Relatório;

(d) Apresentação dos resultados finais; e

(e) Obtenção do aceite formal quanto às entregas realizadas.

3. *Escopo e Regras de Negócios*

Para a execução desse relatório, consideramos a obtenção e verificação de todas as regras de negócio, limitadas ao escopo de nosso trabalho, que são estabelecidas nas legislações, listadas a seguir, referente aos serviços de transporte coletivo de passageiros na região do município do Rio de Janeiro:

- **Lei Municipal nº 5.211/10, regulamentada pelo Decreto nº 32.842/10**

  Institui o bilhete único nos serviços de transporte coletivo municipal do Rio de Janeiro e dá outras providências.

- **Lei Estadual nº 4.291/04**

  Institui o Sistema de Bilhetagem Eletrônica nos serviços de transporte coletivo de passageiros por ônibus, e dá outras providências.

- **Lei Municipal nº 3.167/00**

  Assegura o exercício das gratuidades no Sistema de Bilhetagem Eletrônica e dá outras providências. Cotistas, bolsistas do ProUni e universitários com renda de até um salário mínimo *per capta* residentes no município têm direito a gratuidade, sendo revalidado semestralmente (Art. 2º do Decreto 38.280/14);

- **Decreto n.º 33.975 de 14 de junho de 2011;**

  Altera o Decreto Nº 32.842, de 1º de outubro de 2010, que regulamenta a Lei nº 5.211, de 01 de julho de 2010, que institui o Bilhete Único no Município do Rio de Janeiro, bem como a Lei nº 3.167, de 27 de dezembro de 2000, que disciplina a Bilhetagem Eletrônica nos Serviços de Transporte Público de Passageiros do Município do Rio de Janeiro, na forma que dispõe.

- **Decreto nº 38.362 de 11 de março de 2014;**

  Estende o prazo máximo de transbordo nas viagens com o Bilhete Único para duas horas e trinta minutos, alterando o Decreto nº 32.842, de 1º de outubro de 2010, que institui o Bilhete Único Carioca.

- **Decreto nº 38.279 de 29 de janeiro de 2014;**

  Estabelece medidas para o aperfeiçoamento da prestação do Serviço Público de Transporte de Passageiros por Ônibus - SPPO determina o reajuste tarifário, e dá outras providências.

- **Resolução SMTR nº 2476 de 16 de maio de 2014.**

  Dispõe sobre a tarifa de integração do Serviço Público de Transporte de Passageiros por Ônibus – SPPO-RJ, com os serviços de transporte metroviário e ferroviário, através do Bilhete Único Carioca – BUC e das integrações expressas.

4. Resultados Obtidos

4.1. Análise das funcionalidades do Sistema de Bilhetagem Eletrônica (SBE) e Validador

4.1.1. Análise da usabilidade do Sistema de Bilhetagem Eletrônica (SBE)

Usabilidade

Refere-se ao grau de facilidade oferecido ao usuário na aprendizagem da operação de um sistema e/ou *website*[1].

A usabilidade está diretamente relacionada com a interação de sistemas e/ou *websites* com os usuários e por sua vez, depende de aspectos relacionados a seguir que serviram de base para nossa análise e testes realizados.

1. ***Facilidade de aprendizado***

   Tempo e esforço necessários para que os usuários atinjam um determinado nível de desempenho.

2. ***Facilidade de uso***

   Avalia o esforço físico e cognitivo do usuário durante o processo de interação, medindo a velocidade de uso e o número de erros cometidos durante a execução de uma determinada tarefa.

3. ***Acessibilidade***

   Avalia se o *website* é corretamente desenvolvido, de forma que todos os usuários podem ter igual acesso às informações e funcionalidade.

[1] Consideramos para análise das questões de usabilidade, os seguintes *websites*: (a) *cartaoriocard.com.br (Ambiente Valorado)*; (b) *riocard.com (Ambiente Gratuidade)*; e (c) *vt.fetranspor.com.br* (esse último redireciona para o *website* cartaoriocard.com.br e, dessa forma, foi testado no item (a)).

4. *Produtividade*

Avalia se o uso do *website* permite ao usuário ser mais produtivo do que seria se não o utilizasse.

5. *Consistência dos Dados*

Avalia a consistência das informações, ou seja, verifica se as informações contidas no *website* estão corretas.

6. *Suporte*

Avalia a ajuda disponibilizada aos usuários na manipulação do *website*. Pressupõe a existência de "Ajuda Online".

Os itens de usabilidades listados anteriormente foram avaliados no que tange ao seu nível de aderência, conforme melhores práticas de mercado, como (A) – Atende, (AP) – Atende Parcialmente, (N) – Não Atende, conforme a classificação descrita a seguir:

Classificação da Aderência	Descrição
(A) – Atende	Na análise realizada na funcionalidade, verificamos que a mesma existe e está operando de forma adequada.
(AP) – Atende Parcialmente	Na análise realizada na funcionalidade, verificamos que a mesma existe, mas não opera adequadamente ou existe algum tipo de ajuste que poderia ser implementado para melhorar sua operação.
(N) – Não Atende	Na análise realizada na funcionalidade, verificamos que a mesma não existe ou não está habilitada.

Apresentamos nas tabelas a seguir, os resultados obtidos na avaliação de cada item considerado na nossa análise.

1. Facilidade de Aprendizado

Website	*Aderência*	*Situação Atual*	*Recomendação*
(a) cartaoriocard.com.br (Valorado)	(A) – Atende	O *website* é intuitivo, facilitando o aprendizado do usuário. As informações consideradas importantes para o uso do Bilhete Único são disponibilizadas na página principal e nas demais.	Não aplicável.
(b) riocard.com (Gratuidade)	(AP) – Atende Parcialmente	O *website* apresenta as informações de forma pouco estruturada, podendo gerar confusão ao usuário. A disposição das informações também prejudica o desempenho do usuário, uma vez que as informações não estão adequadamente segmentadas, exigindo do usuário um tempo maior para leitura de todas as informações até encontrar a informação desejada.	Dispor as informações de forma estruturada, visando facilitar o entendimento do usuário. *Links* mais utilizados devem ser destacados para facilitar e agilizar a busca de informações.

2. Facilidade de Uso

Website	*Aderência*	*Situação Atual*	*Recomendação*
(a) cartaoriocard.com.br (Valorado)	(AP) – Atende Parcialmente	O *website* não apresenta opções de ajuda em relação ao preenchimento dos formulários *(conforme imagem 1)*.	Informar os campos que são de preenchimento obrigatório, assim como os formatos exigidos dos dados (Ex.: data: dd/mm/aaaa).
		As críticas em relação aos dados informados somente são apresentadas após o envio da solicitação.	Ajustar a disposição das informações dos "Termos de Uso e Comodato".
		Não é possível visualizar todas as informações referentes aos "Termos de Uso" *(conforme imagem 2)* e aos "Termos de Comodato" *(conforme imagens 3)*.	Criar e disponibilizar "Mapa do Site".
		As informações referentes aos principais serviços (Ex.: "aquisição de cartão" e "recarga") estão dispostas de forma clara e fácil de serem encontradas.	
		Não foi identificado um "Mapa do Site" disponível para suporte à navegabilidade.	

Imagem 1 - O website não apresenta opções de ajuda em relação ao preenchimento dos formulários

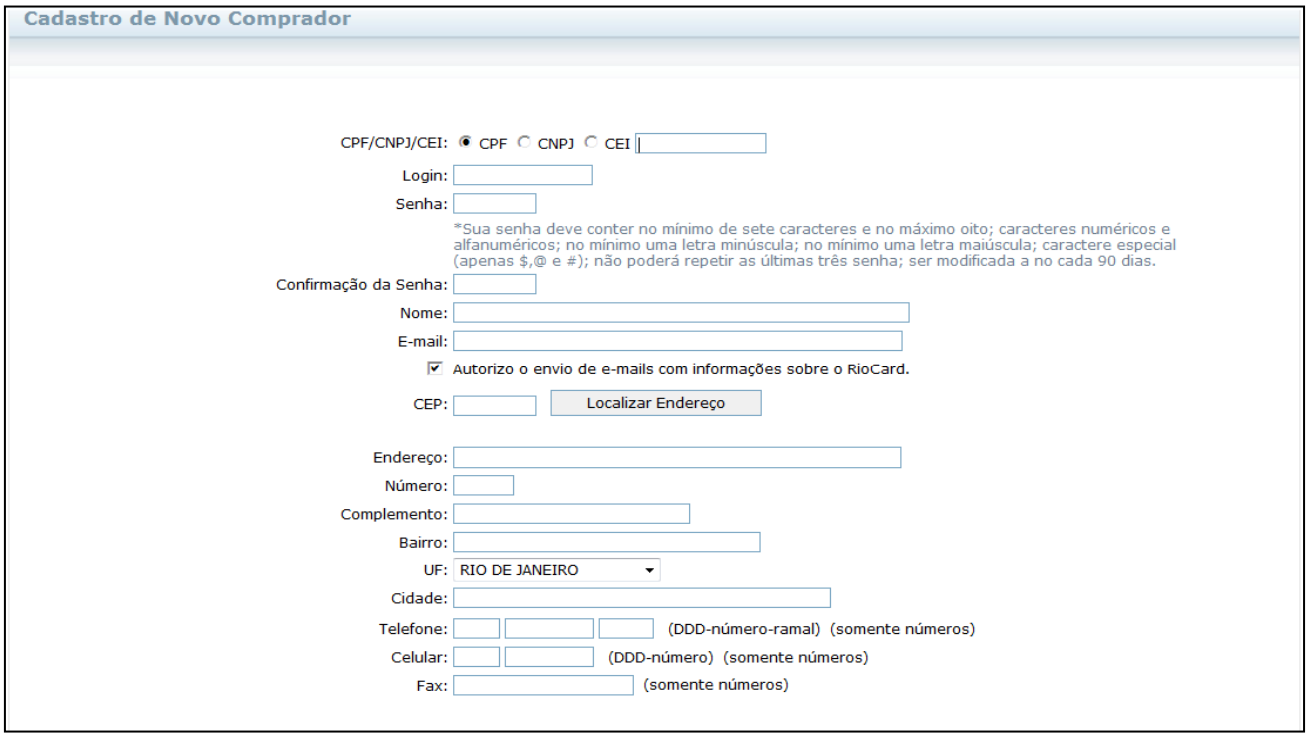

Cadastro de Novo Comprador
CPF/CNPJ/CEI: CPF CNPJ CEI
Login:
Senha:
*Sua senha deve conter no mínimo de sete caracteres e no máximo oito; caracteres numéricos e alfanuméricos; no mínimo uma letra minúscula; no mínimo uma letra maiúscula; caractere especial (apenas $,@ e #); não poderá repetir as últimas três senha; ser modificada a no cada 90 dias.
Confirmação da Senha:
Nome:
E-mail:
Autorizo o envio de e-mails com informações sobre o RioCard.
CEP:
Localizar Endereço
Endereço:
Número:
Complemento:
Bairro:
UF: RIO DE JANEIRO
Cidade:
Telefone: (DDD-número-ramal) (somente números)
Celular: (DDD-número) (somente números)
Fax: (somente números)

Imagem 2 - Não é possível visualizar todas as informações referentes aos "Termos de Uso"

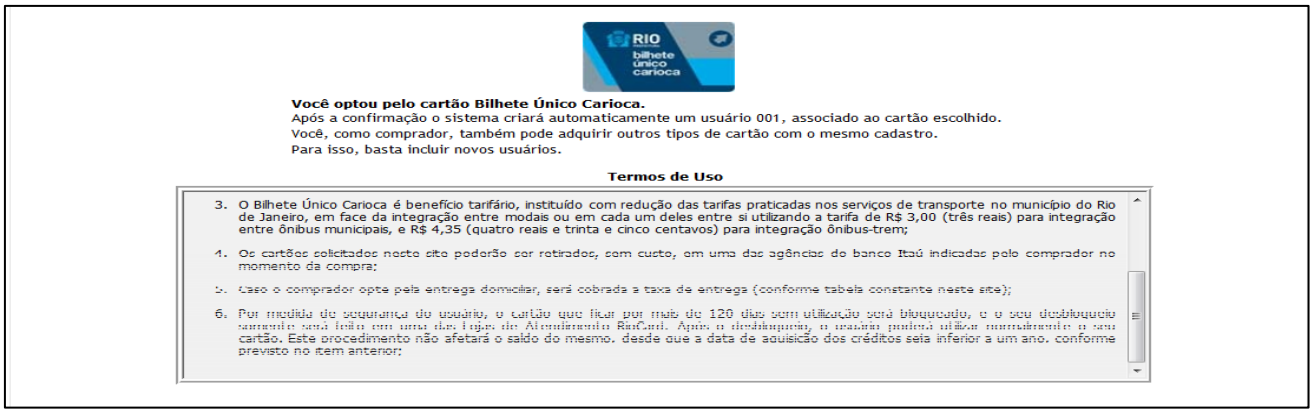
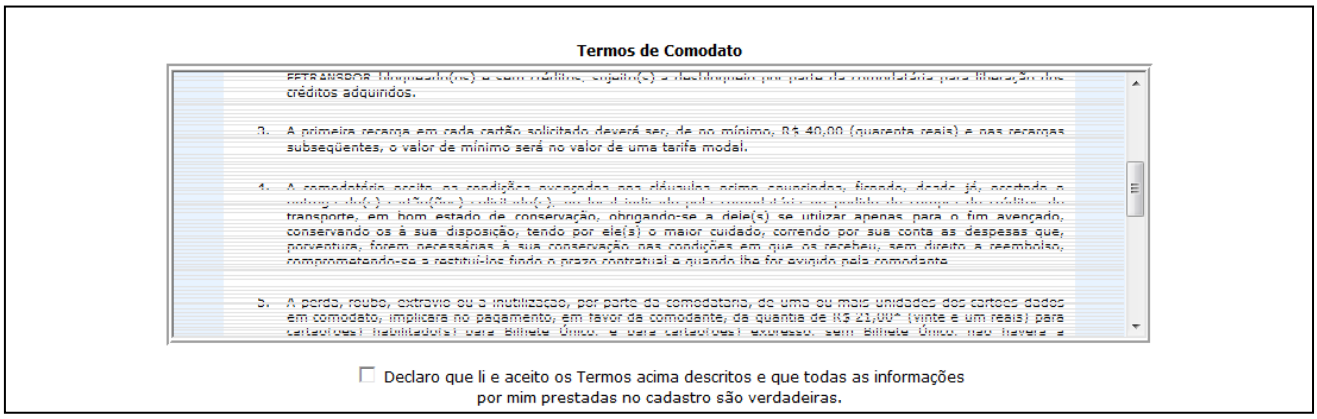

RIO bilhete único carioca
Você optou pelo cartão Bilhete Único Carioca.
Após a confirmação o sistema criará automaticamente um usuário 001, associado ao cartão escolhido.
Você, como comprador, também pode adquirir outros tipos de cartão com o mesmo cadastro.
Para isso, basta incluir novos usuários.
Termos de Uso
3. O Bilhete Único Carioca é benefício tarifário, instituído com redução das tarifas praticadas nos serviços de transporte no município do Rio de Janeiro, em face da integração entre modais ou em cada um deles entre si utilizando a tarifa de R$ 3,00 (três reais) para integração entre ônibus municipais, e R$ 4,35 (quatro reais e trinta e cinco centavos) para integração ônibus-trem;
4. Os cartões solicitados neste site poderão ser retirados, com custo, em uma das agências do banco Itaú indicadas pelo comprador no momento da compra;
5. Caso o comprador opte pela entrega domiciliar, será cobrada a taxa de entrega (conforme tabela constante neste site);
6. Por motivo de segurança do usuário, o cartão que ficar por mais de 120 dias sem utilização será bloqueado, e o seu desbloqueio somente será feito em uma das Lojas de Atendimento RioCard. Após o desbloqueio, o usuário poderá utilizar normalmente o seu cartão. Este procedimento não afetará o saldo do mesmo, desde que a data de aquisição dos créditos seja inferior a um ano, conforme previsto no item anterior;

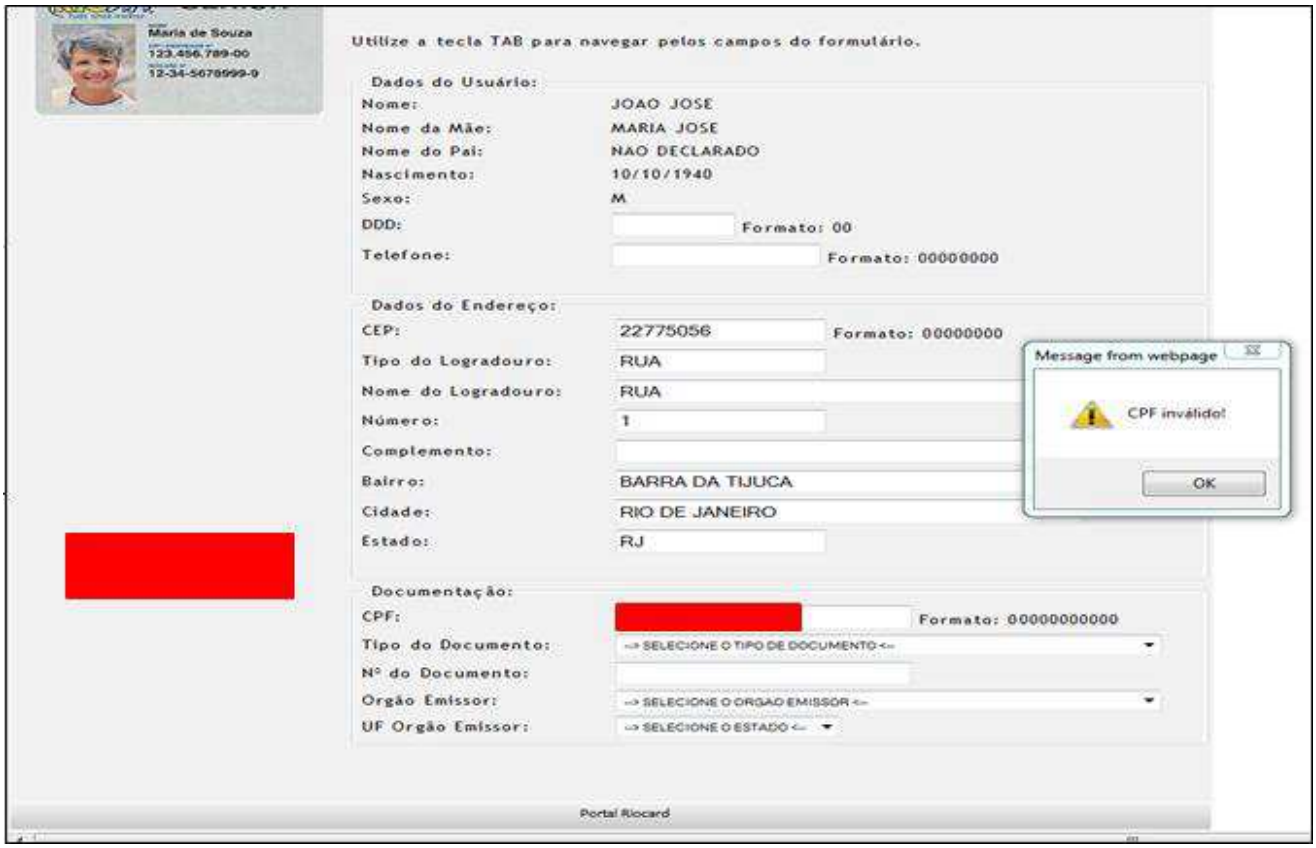
Imagem 3 - Não é possível visualizar todas as informações referentes aos "Termos de Comodato"


Termos de Comodato
créditos adquiridos.
2. A primeira recarga em cada cartão solicitado deverá ser, de no mínimo, R$ 40,00 (quarenta reais) e nas recargas subseqüentes, o valor de mínimo será no valor de uma tarifa modal.
transporte, em bom estado de conservação, obrigando-se a dele(s) se utilizar apenas para o fim avençado, conservando os à sua disposição, tendo por ele(s) o maior cuidado, correndo por sua conta as despesas que, porventura, forem necessárias à sua conservação nas condições em que os recebeu, sem direito a reembolso, comprometendo-se a restituí-los findo o prazo contratual e quando lhe for exigido pela comodante.
5. A perda, roubo, extravio ou a inutilização, por parte da comodatária, de uma ou mais unidades dos cartões dados em comodato, implicará no pagamento, em favor da comodante, da quantia de R$ 21,00^ (vinte e um reais) para cartão(ões) habilitado(s) para Bilhete Único, e para cartão(ões) exonerado, sem Bilhete Único, não haverá a
Declaro que li e aceito os Termos acima descritos e que todas as informações por mim prestadas no cadastro são verdadeiras.

2. Facilidade de Uso (continuação)

Website	*Aderência*	*Situação Atual*	*Recomendação*
(b) riocard.com (Gratuidade)	(AP) – Atende Parcialmente	O *website* apresenta indicações de formato de dados requeridos e indicações de próximos passos, facilitando a sua utilização. O *website* também realiza verificação de CPF quanto à sua validade *(conforme imagem 4)*. Não foi identificado um "Mapa do Site" disponível para suporte à navegabilidade.	Criar e disponibilizar "Mapa do Site".

Imagem 4 - O website também realiza verificação de CPF quanto à sua validade



3. Acessibilidade

Website	*Aderência*	*Situação Atual*	*Recomendação*
(a) cartaoriocard.com.br (Valorado) e riocard.com (Gratuidade)	(N) – Não Atende	Em relação às necessidades visuais, o site não apresenta descrição textual para todas as imagens. Adicionalmente, não existe a possibilidade de ampliar os textos e imagens de modo a facilitar a leitura. Os *links* são destacados através de alteração de cores ou são sublinhados. Não foi identificado nenhum recurso de acessibilidade para usuários com deficiências visuais, auditivas e motoras.	<u>*Para deficientes Visuais*</u> Apresentar descrição textual para todas as imagens. Implementar recursos que possibilite a ampliação de textos e imagens. Utilizar *links* autoexplicativos. Assegurar que o contraste entre as cores de frente e de fundo sejam adequados, de modo a acentuar a possibilidade de leitura para usuários com déficit visual e/ou àqueles com problemas para distinguir cores. <u>*Para deficientes Motores*</u> Implementar *links* e áreas clicáveis maiores, visando facilitar a utilização de pessoas com dificuldades para manusear o mouse. Implementar recursos de codificação do *website* para permitir que os usuários possam navegar utilizando apenas o teclado ou uma única tecla de acesso. <u>*Para deficientes Auditivos*</u> Disponibilizar legendas, ou linguagem de sinais, para todos os vídeos do *website*.

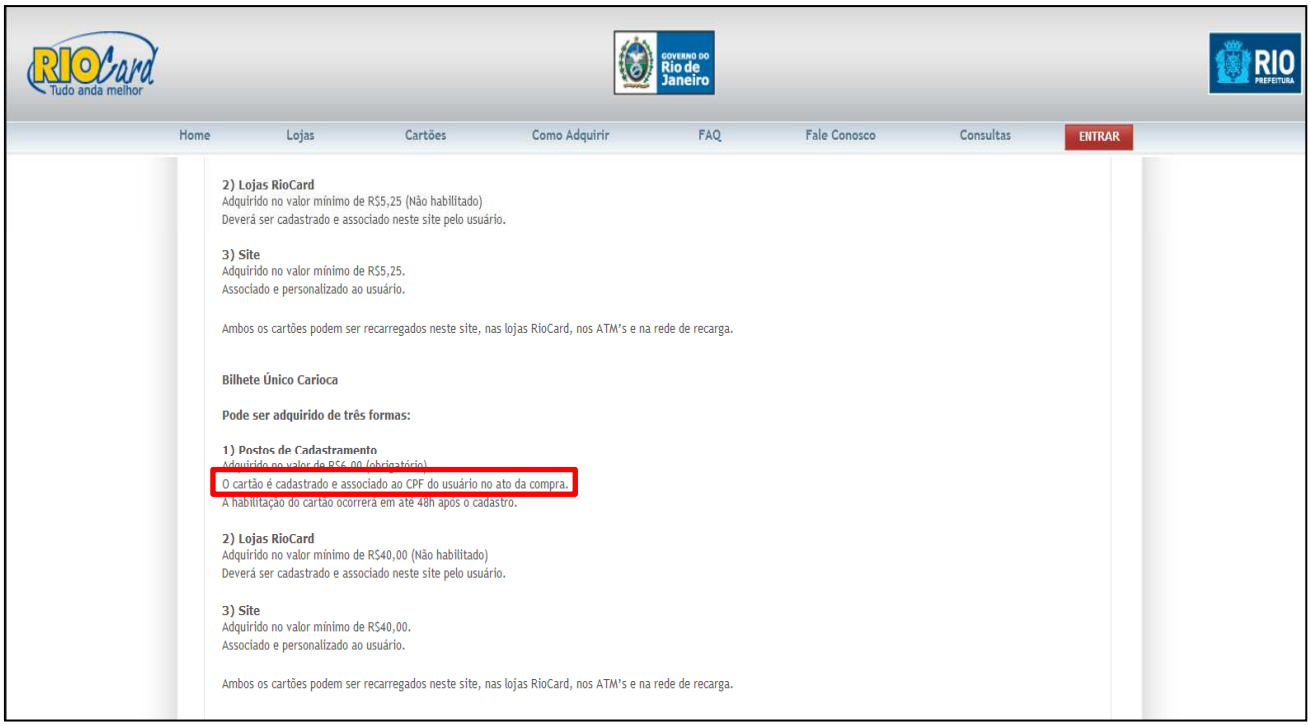
4. Produtividade

Website	*Aderência*	*Situação Atual*	*Recomendação*
(a) cartaoriocard.com.br (Valorado) e riocard.com (Gratuidade)	(A) – Atende	A produtividade do site pode ser facilmente notada, uma vez que, as solicitações realizadas pelo mesmo, trazem uma agilidade em relação a geração da transação sem a sua utilização. A utilização do processo manual deverá ser realizada através do comparecimento em um posto de atendimento.	Não aplicável.

5. Facilidade de Uso

Website	*Aderência*	*Situação Atual*	*Recomendação*
(a) cartaoriocard.com.br (Valorado)	(N) – Não Atende	O *website* apresenta informações inconsistentes no que diz respeito à aquisição de um cartão de Bilhete Único Carioca (BUC), informando ao usuário que o cartão precisa ser associado a um CPF *(conforme imagem 5)*. Entretanto, o processo não ocorre dessa forma, sendo possível a aquisição de cartões de BUC em estações do BRT, sem a apresentação ou cadastro do CPF.	Revisar as informações apresentadas no *website*.
(b) riocard.com (Gratuidade)	(A) – Atende	Não foram identificadas inconsistências de dados no *website*.	Não aplicável.

***Imagem 5* - O *website* informa ao usuário que o cartão precisa ser associado a um CPF**


RIOCard
Tudo anda melhor
GOVERNO DO Rio de Janeiro
RIO PREFEITURA
Home
Lojas
Cartões
Como Adquirir
FAQ
Fale Conosco
Consultas
ENTRAR
2) Lojas RioCard
Adquirido no valor mínimo de R$5,25 (Não habilitado)
Deverá ser cadastrado e associado neste site pelo usuário.
3) Site
Adquirido no valor mínimo de R$5,25.
Associado e personalizado ao usuário.
Ambos os cartões podem ser recarregados neste site, nas lojas RioCard, nos ATM's e na rede de recarga.
Bilhete Único Carioca
Pode ser adquirido de três formas:
1) Postos de Cadastramento
O cartão é cadastrado e associado ao CPF do usuário no ato da compra.
A habilitação do cartão ocorrerá em até 48h após o cadastro.
2) Lojas RioCard
Adquirido no valor mínimo de R$40,00 (Não habilitado)
Deverá ser cadastrado e associado neste site pelo usuário.
3) Site
Adquirido no valor mínimo de R$40,00.
Associado e personalizado ao usuário.
Ambos os cartões podem ser recarregados neste site, nas lojas RioCard, nos ATM's e na rede de recarga.

6. Suporte

Website	*Aderência*	*Situação Atual*	*Recomendação*
(a) cartaoriocard.com.br (Valorado)	(AP) – Atende Parcialmente	O *website* oferece uma seção intitulada "Perguntas Frequentes" como opção de suporte. e outra seção, intitulada "Fale Conosco", com o número de telefone da central de relacionamento.	Implementar recursos de atendimento online (ex.: chats) para facilitar e agilizar o suporte aos usuários.
(b) riocard.com (Gratuidade)	(N) – Não Atende	Não foi identificado no *website* nenhum recurso de suporte ao usuário, ou ajuda online. Identificamos, apenas o número de telefone da central de atendimento, porém, sem a informação do horário de atendimento.	Implementar recursos de atendimento online (ex.: chats) para facilitar e agilizar o suporte aos usuários. Disponibilizar uma seção de perguntas frequentes, com as respectivas orientações. Apresentar, junto ao número informado da Central de Atendimento, os horários de atendimento.

4.2. Análise de Treinamento

O Processo de Treinamento visa à qualificação dos profissionais para execução das tarefas, a melhoria da produtividade e o crescimento profissional do colaborador. Quanto melhor o treinamento, mais desenvolvido o colaborador se tornará, e esse desenvolvimento deve refletir na Organização, proporcionando aumento de produtividade, através da eficiência e eficácia na execução das atividades, sejam operacionais, sejam gerenciais, e na redução de custos com desperdícios e retrabalhos.

A RioCard possui treinamento interno para a Bilhetagem Eletrônica, visto que, além de se tratar do negócio da Organização, muitos colaboradores não possuem experiência anterior em processo de bilhetagem eletrônica.

Identificamos, através de entrevistas realizadas que, tal treinamento é realizado a todos os novos colaboradores, logo após o processo de contratação e, em alguns casos, aos colaboradores mais antigos, com o objetivo de reciclagem.

O material utilizado para este treinamento é o chamado "Livro do Aluno", que nos foi disponibilizado uma cópia impressa para análise, onde pudemos verificar tratar-se de um material de boa qualidade, completo, com boa didática e representações gráficas.

No entanto, ***não identificamos uma documentação formal do processo de treinamento, com definições de metodologia, objetivos, periodicidade e avaliação dos resultados obtidos***, assim como, também não identificamos documentações de controles que suportem a quantidade e a identidade dos usuários treinados.

Na área de Segurança da Informação (SI), identificamos uma iniciativa de reuniões mensais, envolvendo todos os colaboradores (em diferentes turmas) em um treinamento presencial de aproximadamente 2h (duas horas) de duração, com o objetivo de conscientizar os colaboradores a respeito dos procedimentos de Segurança da Informação da Organização, além de boas práticas e outros assuntos pertinentes à segurança, como: engenharia social, segurança no uso dos correios eletrônicos, senhas seguras, entre outros.

Para os treinamentos realizados à Segurança da Informação (SI), identificamos um material em fase de elaboração. No entanto, assim como no caso de bilhetagem eletrônica, ***não identificamos uma documentação formal do treinamento, com definições de metodologia, objetivos, periodicidade e avaliação dos resultados obtidos.***

Outras iniciativas também foram identificadas, como o Security Day, de responsabilidade da área de Segurança da Informação (SI), a ser realizado com periodicidade de 6 (seis) meses, e os cursos de comportamento e ética profissional, de responsabilidade da área de Recursos Humanos (RH), com periodicidade de 4 (quatro) meses. ***No entanto, essas iniciativas encontram-se em fase de planejamento.***

Não identificamos nenhuma iniciativa de treinamentos para os interlocutores, que são os profissionais das operadoras cuja função é monitorar a transmissão de dados entre os validadores, o servidor de comunicação V3Lan da empresa e o *Data Center* da RioCard.

4.3. Análise da documentação existente do Sistema de Bilhetagem Eletrônica (SBE)

A documentação de um sistema deve ter como foco tudo o que envolve o seu ciclo de vida, desde a implementação, passando pelos testes, até a homologação do sistema em si. Servindo como diretriz às equipes envolvidas, de modo que estas mantenham como objetivo o pleno funcionamento do sistema.

A documentação existente do Sistema de Bilhetagem Eletrônica (SBE) em nível de usuário está baseada no documento "Livro do Aluno", que conforme mencionado anteriormente, é parte integrante do treinamento realizado aos novos colaboradores da RioCard. Nesse material podemos encontrar uma visão geral do Sistema de Bilhetagem Eletrônica, desde uma breve apresentação do setor de transporte do Estado do Rio de Janeiro, passando pelas suas funcionalidades, macroprocesso, infraestrutura e operação e gestão dos dados, até os produtos oferecidos pela RioCard.

Por tratar-se de um sistema já implementado e em pleno funcionamento, nossa análise, quanto à documentação existente do Sistema de Bilhetagem Eletrônica (SBE) em nível técnico, teve como foco a avaliação do atendimento aos seus Requisitos Técnicos e Funcionais.

Os Requisitos Técnicos e Funcionais definem as qualidades globais ou atributos contemplados em um sistema, que nem sempre estão explícitas para o cliente ou usuário, mas devem ser implicitamente compreendidos pelo desenvolvedor ou pela área de Tecnologia da Informação. A omissão destes requisitos técnicos e funcionais pode acarretar em vulnerabilidades no sistema, queda da produtividade dos usuários, falta da integridade dos dados, insatisfação dos usuários, descontinuidade prematura do sistema, entre outras.

Dessa forma, realizamos uma análise dos Requisitos Técnicos e Funcionais do Sistema de Bilhetagem Eletrônica (SBE), baseada nas normas de características de "Qualidade de Software (ISO/IEC 9126)" e de processo de "Desenvolvimento de Software (NBR ISO/IEC 15504)", que estão alinhadas com as melhores práticas de mercado.

Abaixo apresentamos os itens considerados na análise que utilizamos para avaliação do Sistema de Bilhetagem Eletrônica:

1. ***Disponibilidade***

   Capacidade do sistema se manter sempre acessível por meio de mecanismos que previnam e resistam a falhas, garantindo alta disponibilidade dos componentes tecnológicos.

2. ***Performance (Desempenho)***

   Desempenho do sistema, isto é, capacidade do sistema em atender aos usuários sem apresentar lentidão para respostas às requisições simultâneas.

3. ***Escalabilidade***

   Capacidade do sistema se adaptar para suportar às novas necessidades exigidas pelo negócio, a facilidade de integração com outros sistemas e a capacidade de suportar a multiplicidade de informações devido ao crescimento da Organização ou do seu modelo.

4. ***Segurança***

   Capacidade do Sistema em proteger os dados processados, incluindo: (a) proteção contra software malicioso; (b) gestão de contas de usuário; (c) segurança de ativos da informação; (d) integridade dos dados; e (e) Trilhas de Auditoria.

5. ***Suporte Técnico***

   Capacidade de atendimento do fornecedor às demandas da Organização.

Os Requisitos Técnicos e Funcionais foram avaliados no que tange ao seu nível de aderência, conforme melhores práticas de mercado, como (A) – Atende, (AP) – Atende Parcialmente, (N) – Não Atende, conforme a classificação descrita a seguir:

Classificação da Aderência	Descrição
(A) – Atende	Na análise realizada no requisito, verificamos se o mesmo existe e está operando de forma adequada.
(AP) – Atende Parcialmente	Na análise realizada no requisito, verificamos se o mesmo existe, mas não opera adequadamente ou existe algum tipo de ajuste que poderia ser implementado para melhorar sua operação.
(N) – Não Atende	Na análise realizada no requisito, verificamos que o mesmo não existe ou não foi identificado.

Apresentamos nas tabelas a seguir, os resultados obtidos na avaliação de cada item considerado na nossa análise.

1. Disponibilidade

Aderência	*Situação Atual*	*Recomendação*
(A) – Atende	Através do histórico de recuperação do sistema, verificamos que o sistema, desde o inicio da sua implementação, não obteve registro de não operação. Identificamos um SLA (acordo de nível de serviço) vigente para recuperação da operação do sistema em até 24 horas. Em relação à contingência, a estrutura conta com uma redundância, de forma simétrica, entre 2 (dois) *mainframes* no Rio de Janeiro. Identificamos também, um contrato vigente com a IBM garantindo um *storage*, localizado em São Paulo, que é sincronizado com o *mainframe* do Rio de Janeiro através de uma VPN com link de 200MB. Verificamos, além da redundância da base de dados, a redundância dos sistemas e dos códigos-fontes. É importante ressaltar que devido ao fato dos validadores possuírem seu processo de atualização e transmissão de dados em forma *off-line*, problemas ocorridos na RioCard não são capazes de interromper o processo de bilhetagem eletrônica de forma imediata.	Não aplicável.

2. Performance (Desempenho)

Aderência	Situação Atual	Recomendação
(A) – Atende	O processamento dos dados de bilhetagem eletrônica é realizado diariamente através do recebimento de informações transmitidas dos validadores. Sendo que seu processamento pode ocorrer de forma *batch (off line)*, sem necessidade de um processamento *on line*.	Não aplicável.

3. Escalabilidade

Aderência	Situação Atual	Recomendação
(A) – Atende	O sistema é capaz de se adaptar para suportar ao crescimento do volume de transações, mantendo a facilidade de integração com outros sistemas e a capacidade de suportar a multiplicidade das informações. O atual modelo de processamento e a integração *off line* com os validadores, permite um nível de escalabilidade. Verificamos através de informações obtidas com o fabricante dos servidores, que conforme a demanda de processamento aumenta, novos módulos de processamento e memória podem ser instalados, garantindo escalabilidade para atender a demanda que for necessária.	Não aplicável.

4. Segurança

Item Avaliado	Aderência	Situação Atual	Recomendação
4.1. Proteção Contra Software Malicioso	(A) – Atende	Para reforçar a Segurança da Informação (SI) na Organização, e evitar que informações sensíveis sejam expostas indevidamente, a RioCard divulga alertas de conscientização das ameaças de segurança e formas de prevenção, através de folhetos e cartazes. Identificamos, que a equipe de Segurança da RioCard realiza um monitoramento diário, através de uma ferramenta chamada "Splunk", da situação de todas as máquinas com relação ao funcionamento e atualizações dos antivírus. Adicionalmente, um representante da McAfee (fornecedora da solução de antivírus) realiza junto à área de Operações uma vistoria mensal no ambiente tecnológico da RioCard, a fim de verificar se as políticas estão corretamente configuradas e mapear máquinas que eventualmente estejam com o software de antivírus desatualizado.	Não aplicável.

4. Segurança (continuação)

Item Avaliado	*Aderência*	*Situação Atual*	*Recomendação*
4.2. Gestão de Contas de Usuário	(AP) – Atende Parcialmente	Identificamos um processo de recolhimento de assinaturas dos colaboradores para o "*Termo de Uso Aceitável dos Recursos Computacionais e Comunicações*", onde o mesmo reconhece que está de acordo com todas as diretrizes definidas nas normas de segurança. Este processo é executado junto a contratação de novos colaboradores, e anualmente, com todos os colaboradores da RioCard. Nos testes que realizamos, pudemos observar, pelo menos, 1 (um) usuário que recebeu acesso ao ambiente tecnológico da RioCard sem realizar assinatura do termo de responsabilidade de uso. Para o processo de concessão e alteração de acesso de usuários aos recursos de TI (banco de dados, sistema operacional e aplicativos), observamos que nem todos são formalmente solicitados, avaliados e aprovados, conforme procedimentos previamente definidos e documentados.	Reforçar os controles para que todos os usuários dos sistemas de informações assinem tempestivamente o "Termo de Uso Aceitável dos Recursos Computacionais e Comunicação". Reforçar os controles de gestão de acesso de usuários para que todas as alterações aos direitos de acesso (criação, modificações e exclusões) sejam administradas para entrar em vigor no momento adequado, baseado apenas em operações documentadas e autorizadas por indivíduos previamente designados. Reforçar a aplicação de parâmetros de configuração da senha de acesso de usuários relacionados aos sistemas Active Directory e RACF, de forma que estes estejam em conformidade com a Norma de Segurança da Informação da RioCard.

4. Segurança (continuação)

Item Avaliado	*Item Avaliado*	*Item Avaliado*	*Item Avaliado*
4.3. Segurança de Ativos da Informação	(N) – Não Atende	Identificamos uma "Norma de Acesso à Informação" disponibilizada na intranet da RioCard, acessível a todos os colaboradores. Observamos que a norma é clara quando se refere à atribuição do menor privilégio para acesso às informações e dados. No entanto, uma vez que os documentos não são classificados, não é possível definir, de forma transparente, o nível de acesso de cada documento.	Revisar a Norma de Segurança de Ativos que trata do tema "Classificação da Informação", para que este documento contemple as diretrizes de uso e tratamento adequado da informação para cada estágio do seu ciclo de vida (criação, distribuição, destruição, etc), de acordo com sua classificação (restrita, confidencial, pública, etc). Restringir uso, distribuição e acesso físico à informação de acordo com sua classificação.

4. Segurança (continuação)

Item Avaliado	*Item Avaliado*	*Item Avaliado*	*Item Avaliado*
4.4. Integridade dos Dados	(AP) – Atende Parcialmente	Não foi identificado um controle implementado que garanta a integridade dos arquivos que são gerados no SBE e transmitidos aos Validadores. Quanto aos arquivos originados nos Validadores e transmitidos à RioCard, são considerados relevantes apenas os arquivos Lo[2]. Esses arquivos contam com um controle de *função hashing* para garantir a integridade das informações contidas nele.	<u>Arquivos originados no SBE e transmitidos aos validadores</u> Recomendamos a implementação de controles que garantam o registro dos erros de inconsistência e análise da integridade dos arquivos. <u>Arquivos originados nos Validadores e transmitidos à RioCard</u> Não identificamos recomendações de oportunidades de melhoria.
4.5 Trilhas de Auditoria	(N) – Não Atende	Atualmente, o Sistema de Bilhetagem Eletrônica (SBE) apenas armazena logs de transações com os cartões.	O sistema deve ser capaz de armazenar todas as atividades críticas realizadas pelos usuários. Adicionalmente, deve ser criado um processo de revisão e análise dos *logs* de auditoria.

[2] Arquivo Lo: possui informações sobre as *transações valoradas* e *confirmação de recargas* que foram feitas nos cartões durante o serviço.

5. Suporte Técnico

Aderência	*Situação Atual*	*Recomendação*
(A) – Atende	Identificamos que todos os fornecedores, considerados como críticos ao suporte do SBE possuem SLA's (acordos de níveis de serviços) definidos em contratos de modo à atender as demandas do sistema e a manutenção do mesmo. São eles: ✓ IBM – Suporte aos Data Centers; ✓ Telium – Suporte à conexões externas; ✓ YIP – Suporte à conexões de Internet; ✓ Mr. DBA – Suporte aos Bancos de dados; e ✓ S&M Informática – Suporte aos Storages do SBE.	Não aplicável.

4.4. Identificação e análise dos acordos de níveis de serviços (SLA) existentes para o suporte técnico do Sistema de Bilhetagem Eletrônica (SBE)

O pleno funcionamento do Sistema de Bilhetagem Eletrônica (SBE) é suportado por diversos serviços que, atualmente, são prestados por terceiros.

Para monitorar e medir os serviços prestados por esses terceiros são estabelecidos "Acordos de Níveis de Serviços" ou, como também são chamados os "SLA" (*Service Level Agreement*). Trata-se de um acordo formal que permite definir para ambas as partes (cliente e fornecedor) todas as garantias que o provedor de serviço oferece em relação aos serviços que foram contratados, assim como a forma como estes serviços serão medidos, reportados e melhorados continuamente.

A RioCard seleciona os fornecedores de acordo com critérios baseados em uma avaliação técnica e financeira. Realiza a gestão dos contratos e monitora se os serviços estão sendo prestados de acordo com os parâmetros de qualidade contratados, aplicando as ações devidas em casos de descumprimento dos acordos firmados nos contratos.

Com exceção dos fornecedores ***Mr. DBA*** e ***S&M informática***, onde ***não identificamos um controle de monitoramento*** em caso de acionamento dos mesmos, bem como critérios de avaliação e plano de ação para casos de não cumprimento dos acordos de níveis de serviços.

A RioCard considera como "Principais Fornecedores", aqueles cujo os serviços prestados sejam críticos para a continuidade do negócio, ou seja: em casos de indisponibilidade prolongada desses serviços, haveria impactos na continuidade do negócio de Bilhetagem Eletrônica.

Dessa forma, relacionamos abaixo os serviços que são considerados críticos pela RioCard, e os respectivos fornecedores:

- ✓ Manutenção dos Datacenters da RioCard - IBM
- ✓ Links de dados com conexão para diversas operadoras e postos de atendimento - Telium
- ✓ Links de internet com conexão para diversas operadoras e postos de atendimento - YIP
- ✓ Suporte técnico aos bancos de dados do SBE – Mr. DBA
- ✓ Mão-de-obra especializada para operação do Tivoli Storage Management – S&M Informática

Abaixo, podemos observar os Acordos de Níveis de serviços firmados com os "Principais Fornecedores" para os serviços críticos relacionados anteriormente:

Tipo de Serviço monitorado	Fornecedor	Detalhamento do Serviço	Nível de acordo de serviço firmado
Data Centers	IBM	Responsável pela manutenção e funcionamento dos Datacenters (principal e contingência) da RioCard.	Infraestrutura e manutenção: ✓ Dias comerciais: 4 horas ✓ Demais dias: 8 horas
Conexões Externas	Telium	Responsáveis pelo fornecimento de links de dados com conexão para diversas operadoras e postos de atendimento.	*Postos de Atendimento:* ✓ Entre 0h 00min – 6h 00min = 4 horas; ✓ Entre 6h 01min – 10h 00min = 1 hora; ✓ Entre 10h 01min – 16h 00min = 2 horas; ✓ Entre 16h 01min – 20h 00min = 1 hora; ✓ Entre 20h 01min – 23h 59min = 2 horas. *Nas garagens:* ✓ Entre 0h 00min – 6h 00min = 1 hora; ✓ Entre 6h 01min – 10h 00min = 2 horas; ✓ Entre 10h 01min – 16h 00min = 4 horas; ✓ Entre 16h 01min – 20h 00min = 2 horas; ✓ Entre 20h 01min – 23h 59min = 1 hora.
Internet	YIP	Responsáveis pelo fornecimento de links de internet com conexão para diversas operadoras e postos de	4 horas, após abertura do chamado. A solução do problema deverá ser feita em até 06 horas.

Tipo de Serviço monitorado	Fornecedor	Detalhamento do Serviço	Nível de acordo de serviço firmado
		atendimento.	Caso não seja possível o reparo neste tempo, a YIP deverá enviar um laudo técnico, informando o tipo de problema e o tempo de solução para o mesmo.
Banco de dados	MR. DBA	Responsável pelo suporte técnico aos bancos de dados do SBE.	✓ Falhas críticas = 1 hora; ✓ Falhas graves = 2 horas; ✓ Falhas de menor impacto = 4 horas;
Storage	S&M Informática	Responsável pelo fornecimento de mão-de-obra especializada no suporte ao Tivoli Storage Management.	*Atendimento Telefônico* ✓ Dúvidas de operação = 15 minutos ✓ Dúvidas sobre funcionalidades do Tivoli Storage Management = 30 minutos ✓ Dúvidas acerca de funcionalidades = 60 min *Atendimento on-site* ✓ Ocorrências de problemas em horário comercial = chegada[3]: 120 min / solução: 4 horas; ✓ Ocorrências de problemas fora do horário comercial = chegada: 4 horas / solução: 24 horas; ✓ Instalações e/ou trocas programadas de hardware e software = chegada: 24 horas / solução: 48 horas.

[3] Tempo de chegada do especialista nas instalações do cliente dentro do município do Rio de Janeiro.

O relacionamento com cada fornecedor é realizado pelos gerentes da RioCard.

Cada gerente é responsável pelos serviços prestados por terceiros diretamente relacionados à sua área de gestão.

Não identificamos nenhuma documentação com um procedimento padrão que estabeleça critérios de como deve ser feito o relacionamento com os fornecedores. Sendo assim, constatamos que cada gestor estabelece critérios para gerir o relacionamento com o fornecedor relacionado à sua área. Os fornecedores críticos, também chamados de "Principais Fornecedores", são todos gerenciados pela área de infraestrutura da RioCard.

O gestor da área de infraestrutura adota um controle baseado em uma planilha eletrônica, onde relaciona todos os incidentes que envolvem a prestação de serviços de terceiros, no caso, os principais fornecedores. Este controle considera a descrição do incidente, o fornecedor envolvido, e o tempo de solução do incidente. Dessa forma, é possível verificar se determinado fornecedor está prestando o serviço conforme os acordos de níveis de serviços definidos em contrato.

Cada contrato possui um plano de ação definido em caso de descumprimento dos acordos. Adicionalmente, o gerente de infraestrutura realiza uma análise de desempenho mensal de cada fornecedor. O resultado desta análise é apresentada no relatório de performance, o qual é enviado à diretoria mensalmente. A análise deste relatório pode resultar em ações diversas como, por exemplo, aplicações de multas e/ou não renovação de contrato.

Recomendamos que a RioCard estabeleça um documento formal com procedimento padrão a ser seguido no que tange à: (a) definição de critérios para acompanhamento dos serviços prestados pelos fornecedores; (b) classificação dos fornecedores, em relação a sua criticidade; (c) ações adotadas para punir ou alertar fornecedores com relação ao não atendimento de níveis de serviços acordados.

Avaliamos os controles de monitoramento de Acordos de Níveis de Serviços, conforme demonstrado abaixo:

Gestão de Fornecedores

Item Avaliado	*Aderência*	*Situação Atual*	*Recomendação*
Monitoramento dos incidentes e ações tempestivas em caso de descumprimento de SLAs	(AP) – Atende Parcialmente	Identificamos que os critérios de medição e planos de ações em caso de descumprimento dos acordos de níveis de serviços estão definidos em contrato para os fornecedores críticos, com exceção do fornecedor S&M Informática.	Estabelecer, junto à fornecedora S&M Informática, critérios de medição e planos de ações em caso de descumprimento dos SLAs.
Monitoramento periódico de desempenho dos fornecedores críticos	(AP) – Atende Parcialmente	Identificamos que há um controle mensal de avaliação de desempenho dos fornecedores IBM, Telium e YIP. No entanto, não identificamos um processo de avaliação periódica para os fornecedores Mr. DBA e S&M Informática.	Incluir os fornecedores S&M Informática e Mr.DBA no processo de avaliação de desempenho mensal.

4.5. Análise do Sistema Validador

O Validador é um computador de bordo, instalado junto às roletas no interior dos ônibus, em vans, e em estações, como no caso de trens, barcas, metrô, BRT's e Teleféricos.

Possui um leitor pronto para receber informações dos cartões RioCard e também transmitir dados, através de processos de transmissão realizados posteriormente à sua "descarga de dados".

A Estrutura do Validador é similar à de um computador comum, possuindo:

- Processadores

  Circuito integrado responsável por realizar as funções de cálculo e tomada de decisão do Sistema Validador.

- Relógio, via bateria

  O relógio do Validador funciona através de uma bateria de lítio, acoplada a placa principal do equipamento. Dessa forma, sendo capaz de manter o horário correto, mesmo quando não houver alimentação elétrica externa.

- Dispositivos de entrada e saída

  Os dispositivos de entrada e saída permitem a interação do equipamento com o homem, ou outros equipamentos. No caso do Validador são considerados dispositivos de entrada e saída, o display; o Sensor (de leitura e escrita nos cartões); a antena Wi-Fi; e o modem GPRS (no caso das vans). Através destes dispositivos, o Validador recebe e envia dados.

- Memória.

  Os módulos de memória instalados nos Validadores permitem o armazenamento dos dados das transações realizadas, assim como o armazenamento das Regras de Negócio vigentes, como integrações, matrizes de linhas, valores de tarifas, e etc.

O Validador é ligado ao sistema elétrico dos ônibus e Vans, ou à rede elétrica das estações. Mesmo com os ônibus e vans desligados, as informações continuam armazenadas na memória interna do Validador, que por sua vez é capaz de armazenar varias informações, dentre eles podemos destacar:

- Parâmetros do sistema

  Parâmetros de configuração do sistema Validador, e outras informações como versões de código, data e hora, e etc.

- Recargas de cartões valorados

  Relação de cartões a serem recarregados e os respectivos valores de recargas, conforme transmitido pela RioCard.

- Hotlist de cartões cancelados

  Relação de cartões a serem cancelados, conforme transmitido pela RioCard.

- Créditos para uso de cartões

  Relação de créditos a serem realizados em novos cartões, conforme transmitido pela RioCard.

- Relação de linhas válidas

  Relação de linhas válidas que servirá de parâmetro na abertura do sistema Validador, garantindo que o mesmo estará associado à uma dessas linhas (válidas).

- Versões de programa

  Informações sobre a versão atual do código, e possíveis versões de atualização do sistema.

- Registro de transações (valoradas, gratuidades, funcionais e operacionais)

  Registro completo das transações realizadas em um Validador, incluindo data e hora da transação, cartão que realizou a transação, valor de tarifa, integrações e etc.

- Matriz de integrações

  Matriz contendo as possibilidades e valores dos vários tipos de integrações que o sistema permite.

No interior de cada Validador existe um *chip* chamado "*chip SAM*". É ele que torna possível o reconhecimento dos cartões RioCard. As informações nele contidas são codificadas, de forma que, sua leitura só seja possível por pessoas autorizadas. Essa é uma medida fundamental para a segurança do sistema.

A fabricação, comercialização e suporte dos equipamentos Validadores são realizados pela PRODATA[4], que mantém diversos contratos com as diversas operadoras e concessionárias de transporte público do estado do Rio de Janeiro.

A RioCard não possui nenhuma participação, ou qualquer tipo de envolvimento no relacionamento entre as operadoras/concessionárias e a PRODATA. ***Esse modelo pode gerar alguns riscos relacionados à gestão descentralizada dos equipamentos e atualizações de versões de regras de negócios. Existem diversas versões do equipamento no mercado, que também exige da RioCard um maior esforço na padronização do desenvolvimento de atualizações.***

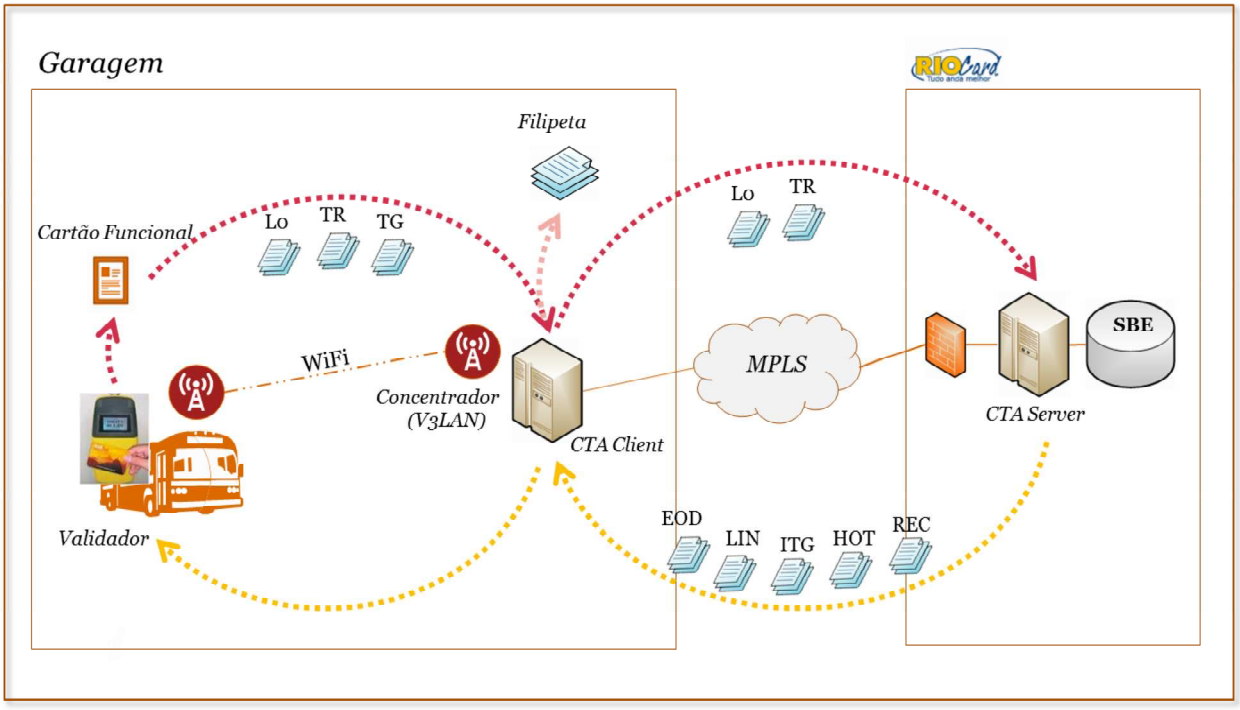
Adicionalmente, o modelo descentralizado de contratos pode representar uma falta de ganho no valor de compra relacionado ao seu volume.

Conforme a tecnologia avança, novas versões de Validadores são lançadas no mercado, com novas funcionalidades como GPS (*Global* Positioning System), GPRS (*General Packet Radio Services*), *upgrade* de memória, integração com impressoras e teclados, identificador biométrico, e etc.

[4] PRODATA: empresa fornecedora dos validadores.

4.5.1. *Identificação e Análise dos controles existentes no Sistema Validador*

Com exceção do código do sistema, todas as outras informações existentes no sistema Validador estão contidas em arquivos, alguns gerados pelo próprio Sistema Validador, e outros gerados pela RioCard, e recebidos através dos servidores/concentradores (vide ilustração abaixo):



Relacionamos abaixo, os arquivos gerados pelo Sistema Validador, e quais informações estão contidas em cada um deles:

✓ Arquivos recebidos do validador, contendo:

- Arquivo Lo: possui informações sobre as ***transações valoradas*** e ***confirmação de recargas*** que foram feitas nos cartões durante o serviço;
- Arquivo TR: possui informações sobre ***transações de gratuidade***; e
- Arquivo TG: possui informações sobre ***vendas a bordo*** (esse arquivo ***não é enviado à RioCard***).

Os arquivos Lo e TR são gerados durante o processo de fechamento do validador e transmitidos aos servidores/concentradores das garagens (no caso das Vans, os arquivos são transmitidos, via GPRS[5], a um concentrador localizado no ambiente interno da RioCard), sendo posteriormente transmitidos para o *Data Center* da RioCard.

Os arquivos nos formatos TG são encontrados apenas nas garagens, pois são os únicos que possuem valores de venda a bordo.

Dessa forma, identificamos alguns controles aplicados aos arquivos que tem como objetivo garantir a integridade e autenticidade dos mesmos, e dos dados neles contidos.

A seguir apresentamos os controles avaliados e recomendações para melhoria dos mesmos, caso seja aplicável.

[5] **GPRS** é a sigla de *General Packet Radio Services*, ou **Serviços Gerais de Pacote por Rádio**. GPRS é uma tecnologia que tem o objetivo de **aumentar as taxas de transferência de dados entre celulares/máquinas de cartões**, facilitando a comunicação e o acesso a redes.

1. *Integridade das informações do cartão; passagens; e validador*

Item Avaliado	*Situação Atual*	*Recomendação*
Função de *Hashing*	Identificamos que os arquivos "Lo" originados no Validador e transmitidos para o SBE, contam com um controle de função *hashing* para garantir a integridade das informações contidas nele. A função *hashing* funciona da seguinte forma: 1) Durante a geração do arquivo, o validador calcula o valor do *hash* com base em seu conteúdo. Essa informação é armazenada no cabeçalho (*header*) do mesmo arquivo, e enviada à RioCard. 2) Já na RioCard, o SBE refaz o cálculo do *hash*, utilizando o mesmo algoritmo que o Validador e confronta com o *hash* apresentado no cabeçalho do arquivo. 3) Quando os valores de *hash* conferem, o arquivo Lo é processado pelo SBE. Quando são divergentes, o SBE recusa o recebimento e notifica o COC (Central de Operações e Controle), que investiga a possível causa do problema. Desta forma, a RioCard garante a integridade do arquivo e dos dados contidos nele.	Sugerimos que seja feita uma análise de risco, sendo formalizada a necessidade ou não de aplicação da *função hashing* nos outros arquivos que são transmitidos entre o Sistema de Bilhetagem Eletrônica (SBE) e Validador. É importante ressaltar que um dos maiores riscos de impacto na segurança do processo de Bilhetagem Eletrônica poderá ser associado quando da captura ou alteração (corromper) dos arquivos transacionais entre SBE e Validador.

2. *Autenticidade das informações do cartão; passagens; e Validador*

Item Avaliado	*Situação Atual*	*Recomendação*
Assinatura Digital	Identificamos que os arquivos originados nos Validadores e transmitidos ao SBE são binários e encapsulados nos próprios Validadores. Identificamos também, a presença de controles de assinatura digital nos sistemas Validadores, permitindo à RioCard verificar a autenticidade (origem) dos arquivos recebidos.	Não Aplicável

3. *Integridade e Autenticidade das informações de recargas*

Item Avaliado	*Situação Atual*	*Recomendação*
Identificador (ID) de recarga	Identificamos que o Sistema Validador conta com um controle que tem por objetivo garantir a não realização de recargas duplicadas. O ID da última recarga é gravado no cartão, no momento em que o mesmo realiza a recarga. Caso o mesmo cartão seja utilizado em outro validador, este verifica o ID da última recarga antes de fornecer uma nova. Caso o ID seja o mesmo, o Validador entende que aquela recarga já foi liberada no cartão, não a realizando novamente.	Não Aplicável

4. *Integridade e Autenticidade do código dos sistemas*

Item Avaliado	*Situação Atual*	*Recomendação*
Gestão de Mudanças para o sistema Validador	Observamos o fluxo de "Gestão de Mudanças" e não identificamos políticas e procedimento formalizados que determine as práticas adequadas para o processo de gestão de mudanças. As avaliações quanto ao impacto e risco das mudanças são realizadas, mas não são formalmente documentadas. Não identificamos políticas e procedimentos documentados que determine as práticas adequadas para as avaliações de impacto e risco das mudanças. Não identificamos documentação que formalize as práticas e critérios adequados para priorização das mudanças, embora essas priorizações, geralmente, são definidas junto às reuniões do comitê gestor de mudanças realizadas na RioCard. Não identificamos políticas e procedimentos documentados que determinem as diretrizes e responsabilidades pelas aprovações de mudanças. Não identificamos políticas e procedimentos documentados que determinem os critérios para classificação de mudanças emergenciais, como também para instruir sobre as práticas adequadas de gestão de mudanças emergenciais. Não identificamos políticas e procedimentos documentados que determinem as práticas adequadas para a autorização, monitoramento e revogação de acessos temporários para tratamento de mudanças.	Estabelecer uma Norma e procedimentos de Gestão de Mudanças, definindo aspectos como: • Avaliação dos riscos envolvidos; • Critérios para priorização das mudanças; • Governança sobre as mudanças; • Critérios para classificação de mudanças emergenciais; • Tratamento de mudanças emergenciais; e • Processo de monitoramento contínuo das mudanças.

5. Distorções/Divergências identificadas e recomendações sugeridas

Nesta seção detalhamos as deficiências/divergências relacionadas aos itens avaliados e que foram apresentados no decorrer desse relatório.

5.1. Identificação e Análise dos controles existentes que garantam integridade e autenticidade das informações de usuários do Sistema de Bilhete Único (BU)

1. Usuários de cartões valorados do Sistema de Bilhetagem Eletrônica, com cadastro pessoal realizado ou não, habilitado para realizar integrações de Bilhete Único Carioca

Riscos	*Situação Atual*	*Recomendação*
Processamento de transações de cartões não homologados.	Na amostra de 27.026.218 registros de transações valoradas, foram identificados 218.989 transações realizadas por 23.797 cartões que não foram identificados na base de cartões valorados fornecida pela RioCard.	Recomendamos a implementação de um controle no SBE que possibilite a identificação de transações realizadas com cartões que não constam na base de cartões ativos do SBE, gerando um registro de incidente a ser tratado.
Gasto excessivo com aquisição e produção de cartões.	Na base de cartões valorados, com 3.564.349 cartões ativos e associados registrados, foram identificados 135.100 cartões cujo campo "CPF" não apresenta nenhum valor (em branco).	Recomendamos que o CPF seja utilizado como campo chave nos registros, facilitando a revisão da base para garantir que cada usuário tenha apenas um cartão.

2. *Usuários de cartões de gratuidades do Sistema de Bilhetagem Eletrônica*

Riscos	*Situação Atual*	*Recomendação*
Uso de cartões de gratuidade não homologados.	Na amostra de 5.215.031 registros de transações de gratuidade, foram identificados 3.452 transações realizadas por 453 cartões que não foram identificados na base de cartões de gratuidade fornecida pela RioCard.	Recomendamos a realização de uma verificação periódica, para os cartões que realizaram transações de gratuidade e não estão na base cadastral, com o objetivo de identificar se os usuários desses cartões são de fato elegíveis ao benefício. Para os casos onde os usuários são elegíveis, é necessário cadastra-los. E para os casos onde os usuários não são elegíveis, o benefício deve ser revogado.
Uso indevido de cartão de gratuidade sênior.	Na base de cartões de gratuidade, com 2.372.584 cartões registrados, foram identificados 582 cartões ativos associados a usuários, cujo campo "Data de Nascimento" não consta nenhum valor (em branco). Foram identificados outros 334 cartões ativos do tipo sênior concedidos a beneficiários com idade inferior a 65 (sessenta e cinco) anos.	Recomendamos que seja implementado controles de validação antes da concessão do benefício, visando garantir que o benefício será concedido apenas para pessoas elegíveis. Adicionalmente, é recomendável revisar periodicamente a base cadastral de gratuidades com o propósito de identificar casos de não elegibilidades e tomar as ações necessárias.

2. Usuários de cartões de gratuidades do Sistema de Bilhetagem Eletrônica (continuação)

Riscos	Situação Atual	Recomendação
Uso de cartão de gratuidade por pessoas diferentes do beneficiário.	Na base de cartões de gratuidade, com 2.372.584 cartões registrados, foram identificados 22.009 cartões ativos, cujos usuários constam com os CPFs cancelados na base da Receita Federal, associados a óbitos, de acordo com o sistema de óbitos (SisObi) utilizado pelos cartórios e mantidos pela DataPrev. Identificamos também que, 293 destes cartões, foram utilizados na amostra de transações analisadas (24 à 30.08.2014), totalizando 2.576 transações.	Recomendamos que seja implementado um controle periódico onde a SMTR, através de convênio com a Dataprev, forneça a relação de registros de óbitos à RioCard. Para que esta sensibilize o sistema SBE de forma a cancelar os cartões associados aos CPFs com registro de óbito.
Uso de cartões de gratuidade após o cancelamento.	Na amostra de 5.215.031 registros de transações de gratuidade, foram identificados 2.545 transações realizadas por 862 cartões que constavam como "inativos" na base de cartões de gratuidade.	Recomendamos que sejam implementados controles que possam garantir o cancelamento dos cartões de gratuidade de forma tempestiva, e que seu uso seja efetivamente impossibilitado.
Concessão de mais de um cartão de gratuidade a uma pessoa.	Na base de cartões de gratuidade, com 2.372.584 cartões registrados, foram identificados 24.648 beneficiários (CPFs) com mais de um cartão ativo associado. Sendo que, um único CPF possui mais de um benefício de gratuidade, em alguns casos, com o mesmo tipo de gratuidade.	Recomendamos a realização de uma verificação periódica, com o objetivo de identificar se os portadores desses cartões são, de fato, elegíveis ao benefício de gratuidade, habilitando apenas um cartão de gratuidade para cada usuário. Adicionalmente, recomendamos que seja implementado um controle automático de verificação de CPFs cadastrados, com o objetivo de impedir que o mesmo CPF seja cadastrado mais de uma vez para emissão de cartões adicionais de gratuidade.

2. Usuários de cartões de gratuidades do Sistema de Bilhetagem Eletrônica (continuação)

Riscos	*Situação Atual*	*Recomendação*
Inconsistência dos dados pessoais dos usuários.	Na base de cartões de gratuidade, com 2.372.584 cartões registrados, foram identificados 17.010 cartões ativos associados à CPFs inválidos (considerando erros de cálculo do dígito verificador, ou caracteres inválidos).	Recomendamos que o sistema onde são cadastrados os CPFs possua a função para validação do digito verificador, com o objetivo de fornecer um nível maior de confiabilidade das informações cadastradas.

5.2. Identificação e Análise dos controles existentes que garantam integridade e autenticidade das informações de passagens, recargas de bilhetes, e pagamentos realizados pela RioCard

1. Controles que garantem integridade, autenticidade e o não repúdio das informações

Riscos	*Situação Atual*	*Recomendação*
Alteração indevida em arquivos gerados no SBE.	Não foi identificado controles de verificação de integridade dos arquivos originados no SBE e enviados aos Validadores.	Recomendamos a implementação de controles para garantir o registro e análise da integridade dos arquivos originados no SBE e enviados ao validador.
Interceptação e alteração de arquivos gerados no SBE.	Não foram identificados controles que garantam a autenticidade dos arquivos gerados pelo SBE e transmitidos aos Validadores.	Recomendamos a elaboração de controles como: Assinatura Digital baseada em chave pública/privada, para garantir a autenticidade dos arquivos (Ex.: EOD, LIN, ITG, lista de recargas e hotlists) gerados no SBE e enviados ao Validador.
Recargas válidas não serem reconhecidas pelo sistema em tempo hábil.	Identificamos que o SBE possui todo o histórico de recargas feitas para cada cartão.	Não Aplicável

Anexo A - Glossário

Para garantir o correto entendimento das informações apresentadas neste relatório e evitar interpretações divergentes ocasionadas por definições diversas para um mesmo termo, apresentamos um glossário técnico que visa determinar os conceitos oficiais adotados para o projeto em questão:

Sistema de Bilhetagem Eletrônica (SBE)

Sistema por meio de cartões eletrônicos (bilhete eletrônico) pelo qual são efetuados os pagamentos no âmbito do sistema de transportes do Estado do Rio de Janeiro. É a ferramenta tecnológica gerida e operada pela RioCard TI, que suporta a operação do Sistema de Bilhete Único Municipal e Intermunicipal.

Usuário Cadastrado

Qualquer cidadão portador de um cartão eletrônico válido e que tenha preenchido o cadastro no Sistema de Bilhetagem Eletrônica.

Usuário Ativo

Usuário Cadastrado que já tenha realizado o desbloqueio do cartão eletrônico por meio da utilização do cartão eletrônico no Validador.

Validador

Aparelho instalado em cada veículo ou em estações de embarque para leitura do cartão eletrônico dos usuários e registro da transação. O Validador pode estar embarcado, ou seja, instalado em veículos dos modais Ônibus e Vans, ou fixo em terminais de embarque, no caso dos aparelhos instalados nas catracas das estações de Barcas, Metrô e Trem.

Transação

Cada registro de viagem realizada, no momento em que o usuário utiliza o cartão eletrônico em um validador, seja instalado em veículos, ou em terminais de embarque.

Viagem

Trajeto percorrido desde a origem até o destino. Ex.: Trajeto realizado desde o bairro de Icaraí, na cidade de Niterói até o centro da cidade do Rio de Janeiro. Este trajeto corresponde a 1 (uma) viagem, mas que pode possuir mais de uma Transação envolvida, quando da realização de integrações ao longo da viagem.

Concessionários e Permissionários

Empresas privadas que adquiriram junto ao Estado o direito de explorar o serviço público de transporte.

Risco

Eventos ou condições incertas relacionadas ao ambiente de TI do sistema de bilhetagem que caso se materializem, poderão impactar a regra de negócio/subprocesso.

Objetivo de Controle

Procedimentos e metas necessários para mitigar os riscos mencionados.

Oportunidade de Melhoria

Percepção de uma necessidade de melhoria, para atendimento de um ponto de atenção identificado nos processos e regras de negócio avaliadas.

© 2014 PRICEWATERHOUSECOOPERS CORPORATE FINANCE & RECOVERY LTDA. Todos os direitos reservados. Neste documento, "PwC" refere-se à PRICEWATERHOUSECOOPERS CORPORATE FINANCE & RECOVERY LTDA, a qual é uma firma membro do network da PricewaterhouseCoopers International Limited, sendo que cada firma membro constitui-se em uma pessoa jurídica totalmente separada e independente. O termo "PwC" refere-se à rede (network) de firmas membro da PricewaterhouseCoopers International Limited (PwCIL) ou, conforme o contexto determina, a cada uma das firmas membro participantes da rede da PwC. Cada firma membro da rede constitui uma pessoa jurídica separada e independente e que não atua como agente da PwCIL nem de qualquer outra firma membro. A PwCIL não presta serviços a clientes. A PwCIL não é responsável ou se obriga pelos atos ou omissões de qualquer de suas firmas membro, tampouco controla o julgamento profissional das referidas firmas ou pode obrigá-las de qualquer forma. Nenhuma firma membro é responsável pelos atos ou omissões de outra firma membro, nem controla o julgamento profissional de outra firma membro ou da PwCIL, nem pode obrigá-las de qualquer forma.

Obrigado!

www.pwc.com.br
&
www.strategyand.pwc.com

© 2014 PricewaterhouseCoopers Corporate Finance & Recovery Ltda. Todos os direitos reservados. Neste documento, “PwC” refere-se à PricewaterhouseCoopers Serviços Profissionais Ltda, a qual é uma firma membro do network da PricewaterhouseCoopers International Limited, sendo que cada firma membro constitui-se em uma pessoa jurídica totalmente separada e independente.

O termo “PwC” refere-se à rede (network) de firmas membro da PricewaterhouseCoopers International Limited (PwCIL) ou, conforme o contexto determina, a cada uma das firmas membro participantes da rede da PwC. Cada firma membro da rede constitui uma pessoa jurídica separada e independente e que não atua como agente da PwCIL nem de qualquer outra firma membro. A PwCIL não presta serviços a clientes. A PwCIL não é responsável ou se obriga pelos atos ou omissões de qualquer de suas firmas membro, tampouco controla o julgamento profissional das referidas firmas ou pode obrigá-las de qualquer forma. Nenhuma firma membro é responsável pelos atos ou omissões de outra firma membro, nem controla o julgamento profissional de outra firma membro ou da PwCIL, nem pode obrigá-las de qualquer forma.

(DC2) Uso Restrito na PwC - Confidencial